TOWARD DETECTION AND ATTRIBUTION OF CYBER-ATTACKS IN IOT-ENABLED CYBER-PHYSICAL SYSTEMS

[1]*DR. U. M. Fernandes Dimlo*, [2]*Yedla Asha*, [3]*Mamudipally Tejaswi*, [4]*Dheeravath Parushu Ram*, [5]*Challagali Deva*

Professor in Department of CSE Sreyas Institute Of Engineering And Technology

[2.3.4,5]UG Scholar in Department of CSE Sreyas Institute Of Engineering And Technology

Abstract

Securing Internet of Things (IoT)-enabled cyber physical systems (CPS) can be challenging, as security solutions developed for general information / operational technology (IT / OT) systems may not be as effective in a CPS setting. Thus, this paper presents a two-level ensemble attack detection and attribution framework designed for CPS, and more specifically in an industrial control system (ICS). At the first level, a decision tree combined with a novel ensemble deep representation learning model is developed for detecting attacks imbalanced ICS environments. At the second level, an ensemble deep neural network is designed for attack attribution. The proposed model is evaluated using real-world datasets in gas pipeline and water treatment system. Findings demonstrate that the proposed model outperforms other competing approaches with similar computational complexity.

KEYWORDS: *cyber physical systems, industrial control system, deep neural network*

I INTRODUCTION

Internet of Things (IoT) devices are increasingly integrated in cyber-physical systems (CPS), including in critical infrastructure sectors such as dams and utility plants. In these settings, IoT devices (also referred to as Industrial IoT or IIoT) are often part of an Industrial Control System (ICS), tasked with the reliable operation of the infrastructure. ICS can be broadly defined to include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and systems that comprise programmable logic controllers (PLC) and Modbus protocols. The connection between ICS or IIoT-based systems with public networks, however, increases their attack surfaces and risks of being targeted by cyber criminals. One high-profile example is the Stuxnet campaign, which reportedly targeted Iranian centrifuges for nuclear enrichment in 2010, causing severe damage to the equipment. Another example is that of the incident targeting a pump that resulted in the failure of an Illinois water plant.

Sensors are most commonly used in numerous applications ranging from body-parameters' measurement to automated driving. Moreover, sensors play a key role in performing detection- and vision-related tasks in all the modern applications of science, engineering and technology where the computer vision is dominating. An interesting emerging domain that employs the smart sensors is the Internet of Things (IoT) dealing with wireless networks and sensors distributed to sense data in real time and producing specific outcomes of interest through suitable processing. In IoT-based devices, sensors and artificial intelligence (AI) are the most important elements which make these devices sensible and intelligent. In fact, due to the role of AI, the sensors act as smart sensors and find an efficient usage for a variety of applications, such as general environmental monitoring monitoring a certain number of environmental factors; weather forecasting; satellite imaging and its use; remote sensing based applications; hazard events' monitoring such as landslide detection; self-driving cars; healthcare and so on. In reference to this latter sector, recently the usage of smart devices has been hugely increased in hospitals and diagnostic centers for evaluating and monitoring various health conditions of affected patients, remotely as well as physically.

Practically, there is no field of science or research which performs smartly without using the modern sensors. The wide usage and need of sensors; and IoT employed in remote sensing, environment and human health monitoring make the applications as intelligent. In the last decade, the agriculture applications have also included the utilization of many types of sensors for monitoring and controlling various types of environmental parameters such as temperature, humidity, soil quality, pollution, air quality, water contamination, radiation, etc. This paper also aims to highlight the use of the sensors and IoT for remote sensing and agriculture applications in terms of extensive discussion and review.

Civil infrastructure get damaged with time, and the reason for the damage is heavy vehicles, loading environmental changes, and dynamic forces such as seismic. These types of changes mainly occur at existing structures constructed long ago, and various methods will detect that damage. The strategy of SHM involves observing the structure for a certain period to notice the condition of the structure and the periodic measurements of data will be collected, and the features of data will be extracted from these computation results, and the process of analysis can be done with the help of a featured data to find out the present-day health of the structure. The information collected from the process can be updated periodically to monitor the structure and based on the data collected through monitoring a structure, and the structure can be strengthened and repaired, and rehabilitation and maintenance can be completed

II LITERATURE SURVEY

\*"Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data,"*

The growing number of attacks against cyber-physical systems in recent years elevates the concern for cybersecurity of industrial control systems (ICSs). The current efforts of ICS cybersecurity are mainly based on firewalls, data diodes, and other methods of intrusion prevention, which may not be sufficient for growing cyber threats from motivated attackers. To enhance the cybersecurity of ICS, a cyber-attack detection system built on the concept of defense-in-depth is developed utilizing network traffic data, host system data, and measured process parameters. This attack detection system provides multiple-layer defense in order to gain the defenders precious time before unrecoverable consequences occur in the physical system. The data used for demonstrating the proposed detection system are from a real-time ICS testbed. Five attacks, including man in the middle (MITM), denial of service (DoS), data exfiltration, data tampering, and false data injection, are carried out to simulate the consequences of cyber attack and generate data for building data-driven detection models.

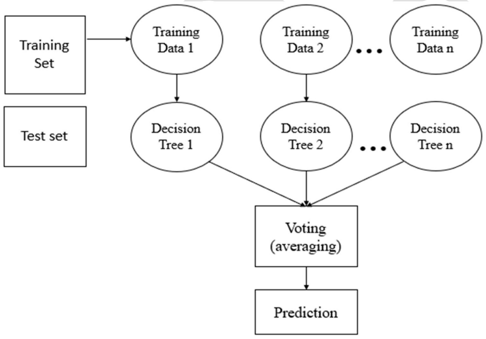
"Stealthy Attack Against Redundant Controller Architecture of Industrial CyberPhysical System"

In an industrial cyber-physical system (iCPS), the controller plays a critical role in guaranteeing reliability and stability. Therefore, redundant controller architecture is a well-adopted approach by distributed control systems (DCS), supervisory control and data acquisition (SCADA), and other typical iCPSs. They monitor and control the critical industrial process, such as power generation, chemical industry, water treatment plant, etc. Redundant controller architecture has been designed and largely implemented in response to unpredictable mechanical failures. However, this structure initially proposed for guaranteeing reliability and safety may expand the cyber-attack surface, posing the risk that an attacker may take advantage of this architecture for stealthy attacks. In this article, we analyze the vulnerability arising from the redundant controller architecture and propose a combined attack methodology against these redundant controller architecture systems in a stealthy manner. We find several 0-day vulnerabilities of the real-world devices from three manufacturers and further implement the combined attack over these devices.

III EXISTING SYSTEM

Random Forest Algorithm

Random Forest is a popular machine learning algorithm that belongs to the supervised learning technique. It can be used for both Classification and Regression problems in ML. It is based on the concept of ensemble learning, which is a process of combining multiple classifiers to solve a complex problem and to improve the performance of the model. As the name suggests, "Random Forest is a classifier that contains a number of decision trees on various subsets of the given dataset and takes the average to improve the predictive accuracy of that dataset." Instead of relying on one decision tree, the random forest takes the prediction from each tree and based on the majority votes of predictions, and it predicts the final output. The greater number of trees in the forest leads to higher accuracy and prevents the problem of overfitting.



Random Forest algorithm

Random Forest algorithm

Step 1: In Random Forest n number of random records are taken from the data set having k number of records.

Step 2: Individual decision trees are constructed for each sample.

Step 3: Each decision tree will generate an output.

Step 4: Final output is considered based on Majority Voting or Averaging for Classification and regression respectively.

Important Features of Random Forest

- **Diversity**- Not all attributes/variables/features are considered while making an individual tree, each tree is different.
- **Immunetothecurseofdimensionality**- Since each tree does not consider all the features, the feature space is reduced.
- **Parallelization**-Each tree is created independently out of different data and attributes. This means that we can make full use of the CPU to build random forests.
- **Train-Testsplit**- In a random forest we don't have to segregate the data for train and test as there will always be 30% of the data which is not seen by the decision tree.
- **Stability**- Stability arises because the result is based on majority voting/ averaging.

Assumptions for Random Forest

Since the random forest combines multiple trees to predict the class of the dataset, it is possible that some decision trees may predict the correct output, while others may not. But together, all the trees predict the correct output. Therefore, below are two assumptions for a better Random forest classifier:

- There should be some actual values in the feature variable of the dataset so that the classifier can predict accurate results rather than a guessed result.
- The predictions from each tree must have very low correlations.

Below are some points that explain why we should use the Random Forest algorithm

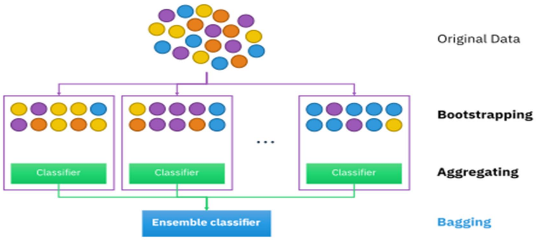
- It takes less training time as compared to other algorithms.
- It predicts output with high accuracy, even for the large dataset it runs efficiently.

- It can also maintain accuracy when a large proportion of data is missing.

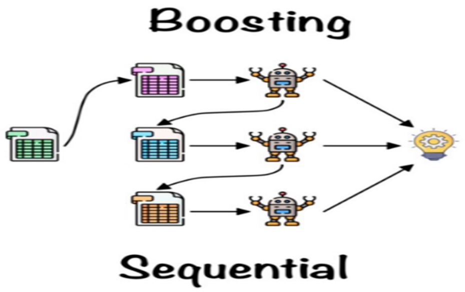
Types of Ensembles

Before understanding the working of the random forest, we must look into the ensemble technique. Ensemble simply means combining multiple models. Thus, a collection of models is used to make predictions rather than an individual model. Ensemble uses two types of methods:

Bagging– It creates a different training subset from sample training data with replacement & the final output is based on majority voting. For example, Random Forest. Bagging, also known as Bootstrap Aggregation is the ensemble technique used by random forest. Bagging chooses a random sample from the data set. Hence each model is generated from the samples (Bootstrap Samples) provided by the Original Data with replacement known as row sampling. This step of row sampling with replacement is called bootstrap. Now each model is trained independently which generates results. The final output is based on majority voting after combining the results of all models. This step which involves combining all the results and generating output based on majority voting is known as aggregation.



RF Classifier analysis



Boosting RF Classifier.

Boosting– It combines weak learners into strong learners by creating sequential models such that the final model has the highest accuracy. For example, ADA BOOST, XG BOOST.

Disadvantages

The Random Forest algorithm, while robust and versatile, does have some disadvantages and limitations that may affect its performance or suitability in certain scenarios. Below are some of the disadvantages associated with the existing system of Random Forest, which may need to be considered in project planning or development:

Complexity and Interpretability: One of the significant disadvantages of the Random Forest algorithm is its complexity, particularly in terms of model interpretation. Each decision tree in the forest considers different attributes and splits over those attributes in various ways. This makes the model as a whole very complex and difficult to interpret compared to simpler models like decision trees, where the decision path can be easily visualized and understood.

Performance on High-Dimensional Data: Despite being immune to the curse of dimensionality to some degree, Random Forest can still suffer from performance issues when dealing with datasets having a very high number of features. The efficiency and effectiveness can degrade as feature space increases, especially when many features are irrelevant or redundant.

Resource Intensiveness: Building multiple decision trees requires more computational resources, including memory and processing power, particularly as the number of trees and the depth of each tree increase. This can lead to higher operational costs and slower processing times, which might be impractical for real-time applications or systems with limited hardware capabilities.

IV PROBLEM STATEMENT

The problem addressed in this project is the security of IoT-enabled cyber-physical systems (CPS), such as industrial control systems, which are vulnerable to cyber-attacks. Traditional security solutions are often ineffective in these settings. The challenge is to create a system that can detect and attribute these cyber-attacks accurately. This project aims to develop a new framework that collects data from various sources within the CPS, uses machine learning to analyze it, and then makes informed decisions on how to respond to potential cyber-attacks. By doing so, it enhances the security of these critical systems and safeguards them against threats from the digital world.

V PROPOSED SYSTEM

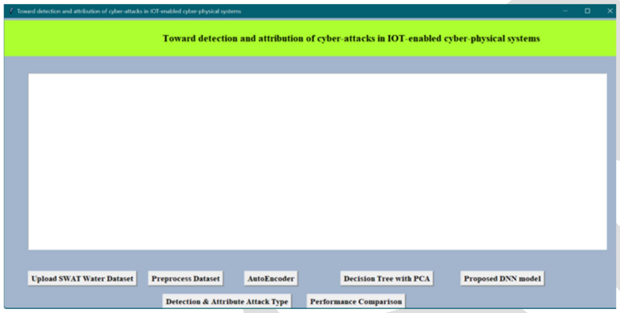
Due to the consideration of both attack and normal data in the training step, the proposed attack detection method can detect previously seen attacks with better f-measures than the other methods, as can be seen in Table I. To enhance the method's ability to face the previously unseen attacks, an anomaly detection module was added to the system trained on the normal data to capture the normal data structure and detect anomalies. The OCSVM model was used in this module. The proposed attack detection component is scalable to larger ICS with more features and larger data sets. The only part of the system that depends on the ICS architecture is the representation-learning step, which needs more training time by increasing the size of the system and/or the data's size. However, it will not affect the performance of the proposed framework in real implementation.

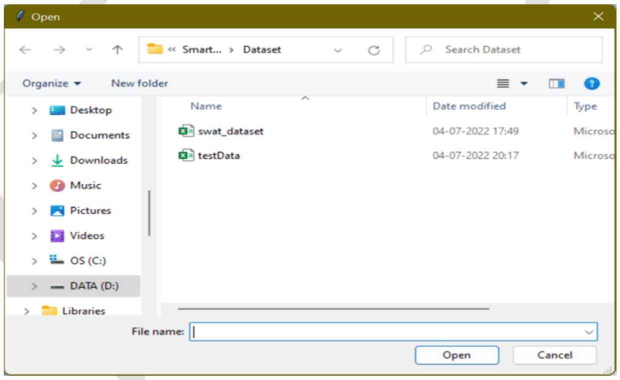
VI IMPLEMENTATION

- Upload SWAT water dataset
- Preprocess dataset
- Run auto encoder algorithm
- Run decision tree with PCA

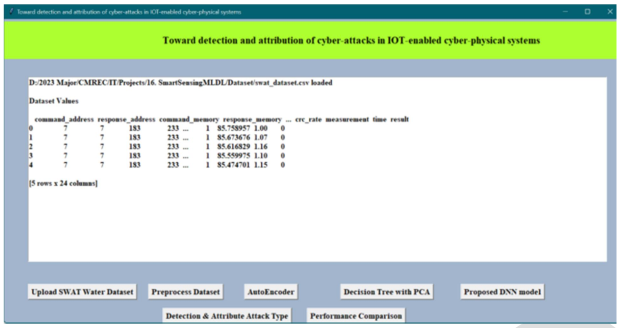
- Run DNN algorithm
- Detection and attribute attack type
- Comparison graph

VII RESULTS

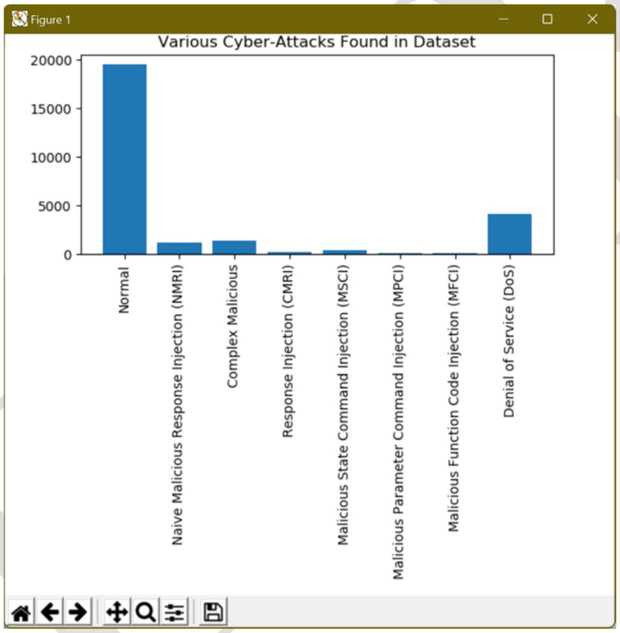

Toward detection and attribution of cyber-attacks in IOT-enabled cyber-physical systems
Toward detection and attribution of cyber-attacks in IOT-enabled cyber-physical systems
Upload SWAT Water Dataset
Preprocess Dataset
AutoEncoder
Decision Tree with PCA
Proposed DNN model
Detection & Attribute Attack Type
Performance Comparison

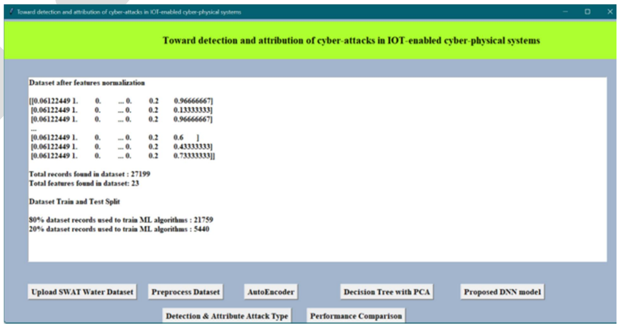


Name	Date modified	Type
swat_dataset	04-07-2022 17:49	Microso
testData	04-07-2022 20:17	Microso

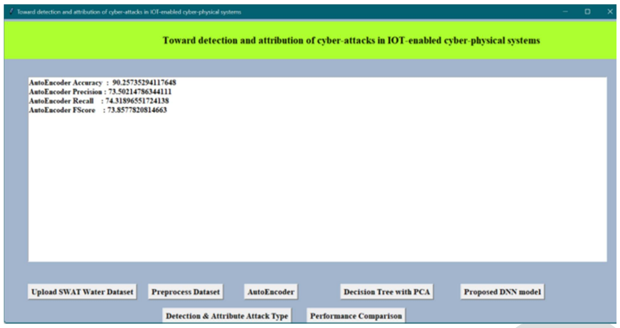

Toward detection and attribution of cyber-attacks in IOT-enabled cyber-physical systems
Toward detection and attribution of cyber-attacks in IOT-enabled cyber-physical systems
Upload SWAT Water Dataset
Preprocess Dataset
AutoEncoder
Decision Tree with PCA
Proposed DNN model
Detection & Attribute Attack Type
Performance Comparison

```
D:/2023 Major/CMREC/IT/Projects/16. SmartSensingMLDL/Dataset/swat_dataset.csv loaded

Dataset Values

  command_address  response_address  command_memory  response_memory  ...  crc_rate  measurement  time  result
0           7               7            183             233  ...         1  85.758957  1.00      0
1           7               7            183             233  ...         1  85.673676  1.07      0
2           7               7            183             233  ...         1  85.616829  1.16      0
3           7               7            183             233  ...         1  85.559975  1.10      0
4           7               7            183             233  ...         1  85.474701  1.15      0

[5 rows x 24 columns]
```

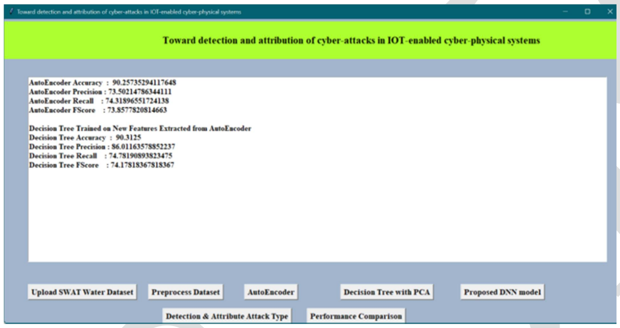



Toward detection and attribution of cyber-attacks in IOT-enabled cyber-physical systems
Toward detection and attribution of cyber-attacks in IOT-enabled cyber-physical systems
Upload SWAT Water Dataset
Preprocess Dataset
AutoEncoder
Decision Tree with PCA
Proposed DNN model
Detection & Attribute Attack Type
Performance Comparison

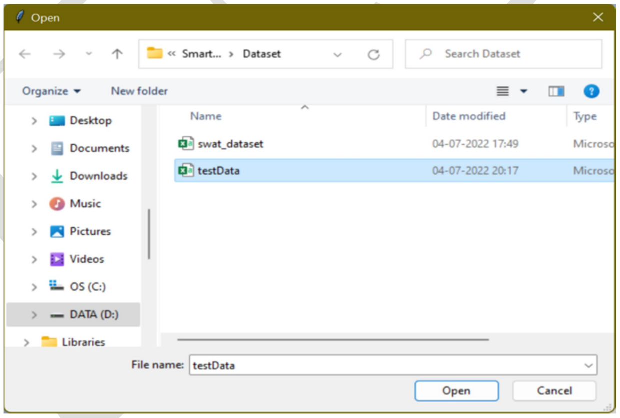
```
Dataset after features normalization

[[0.06122449 1.         0.         ... 0.         0.2        0.96666667]
 [0.06122449 1.         0.         ... 0.         0.2        0.13333333]
 [0.06122449 1.         0.         ... 0.         0.2        0.96666667]
 ...
 [0.06122449 1.         0.         ... 0.         0.2        0.6       ]
 [0.06122449 1.         0.         ... 0.         0.2        0.43333333]
 [0.06122449 1.         0.         ... 0.         0.2        0.73333333]]

Total records found in dataset : 27199
Total features found in dataset: 23

Dataset Train and Test Split

80% dataset records used to train ML algorithms : 21759
20% dataset records used to train ML algorithms : 5440
```


Toward detection and attribution of cyber-attacks in IOT-enabled cyber-physical systems
Toward detection and attribution of cyber-attacks in IOT-enabled cyber-physical systems
Upload SWAT Water Dataset
Preprocess Dataset
AutoEncoder
Decision Tree with PCA
Proposed DNN model
Detection & Attribute Attack Type
Performance Comparison

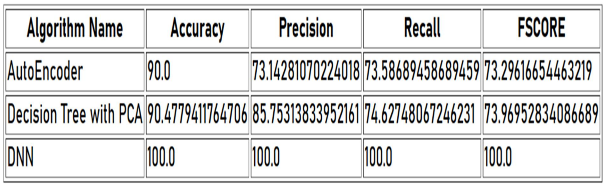
```
AutoEncoder Accuracy  :  90.25735294117648
AutoEncoder Precision : 73.50214786344111
AutoEncoder Recall    : 74.31896551724138
AutoEncoder FScore    : 73.8577820814663
```


Toward detection and attribution of cyber-attacks in IOT-enabled cyber-physical systems
Toward detection and attribution of cyber-attacks in IOT-enabled cyber-physical systems
Upload SWAT Water Dataset
Preprocess Dataset
AutoEncoder
Decision Tree with PCA
Proposed DNN model
Detection & Attribute Attack Type
Performance Comparison

```
AutoEncoder Accuracy  :  90.25735294117648
AutoEncoder Precision : 73.50214786344111
AutoEncoder Recall    : 74.31896551724138
AutoEncoder FScore    : 73.8577820814663

Decision Tree Trained on New Features Extracted from AutoEncoder
Decision Tree Accuracy  :  90.3125
Decision Tree Precision : 86.01163578852237
Decision Tree Recall    : 74.78190893823475
Decision Tree FScore    : 74.17818367818367
```



File name: testData



Algorithm Name	Accuracy	Precision	Recall	FSCORE
AutoEncoder	90.0	73.14281070224018	73.58689458689459	73.29616654463219
Decision Tree with PCA	90.4779411764706	85.75313833952161	74.62748067246231	73.96952834086689
DNN	100.0	100.0	100.0	100.0

VIII CONCLUSION

We introduce a significant machine learning-based classification model (SVM) to identify infected fishes in this research work. The real-world without augmented dataset (163 infected and 68 fresh) and augmented dataset (785 infected and 320 fresh) are used to train our model is new and novel. We mainly classify fishes into two individual classes: fresh fish and another is infected fish. We appraise our model with various metrics and show the classified outcome with visual interaction from those classification results. Besides developing our classifier, we applied updated image process ing techniques like k-means segmentation, cubic spline interpolation, and adaptive histogram equalization for transforming our input image more adaptable to our classifier. We also compare our model results with three classification models and observe that our proposed classifier is the best solution in this case.

This work contributes to bringing out a superior automated fish detection system than the existed systems based on image processing or lower accuracy. We not only depend on the modern image processing technique but also adjoin demandable supervised learning techniques. We prosperously develop the classifier that predicts infected fish with the best accuracy rate than other systems for our real-world novel dataset.

REFERENCES

[1] T. Acharya. Median computation-based integrated color interpolation and color space conversion methodology from 8-bit bayer pattern rgb color space to 24-bit ciexyz color space, 2002. US Patent 6,366,692.

[2] Ben-Hur and J. Weston. A user’s guide to support vector machines. In Data mining techniques for the life sciences, pages 223– 239. Springer, 2010.

[3] S. Bianco, F. Gasparini, A. Russo, and R. Schettini. A new method for rgb to xyz transformation based on pattern search optimization. IEEE Transactions on Consumer Electronics, 53(3):1020–1028, 2007.

[4] E. Bisong. Google colaboratory. In Building Machine Learning and Deep Learning Models on Google Cloud Platform, pages 59–64. Springer, 2019.

[5] P. Bradley. The use of the area under the roc curve in the evaluation of machine learning algorithms. Pattern recognition, 30(7):1145– 1159, 1997.

[6] S. A. Burney and H. Tariq. K-means cluster analysis for image segmentation. International Journal of Computer Applications, 96(4), 2014.

[7] M. A. Chandra and S. Bedi. Survey on svm and their application in image classification. International Journal of Information Technology, pages 1–11, 2018.

[8] L. de Oliveira Martins, G. B. Junior, A. C. Silva, A. C. de Paiva, and M. Gattass. Detection of masses in digital mammograms using kmeans and support vector machine. ELCVIA Electronic Letters on Computer Vision and Image Analysis, 8(2):39–50, 2009.